2018年
2月
FEBRUARY

MALWARE REPORT

マルウェアレポート

国内のマルウェア検出状況を解説

Web ブラウザー上の脅威を多く観測

キヤノン IT ソリューションズ株式会社

はじめに

「マルウェアレポート」は、キヤノンITソリューションズが運営する

「マルウェアラボ」が「ESETセキュリティ ソフトウェア シリーズ」の検出データを基に

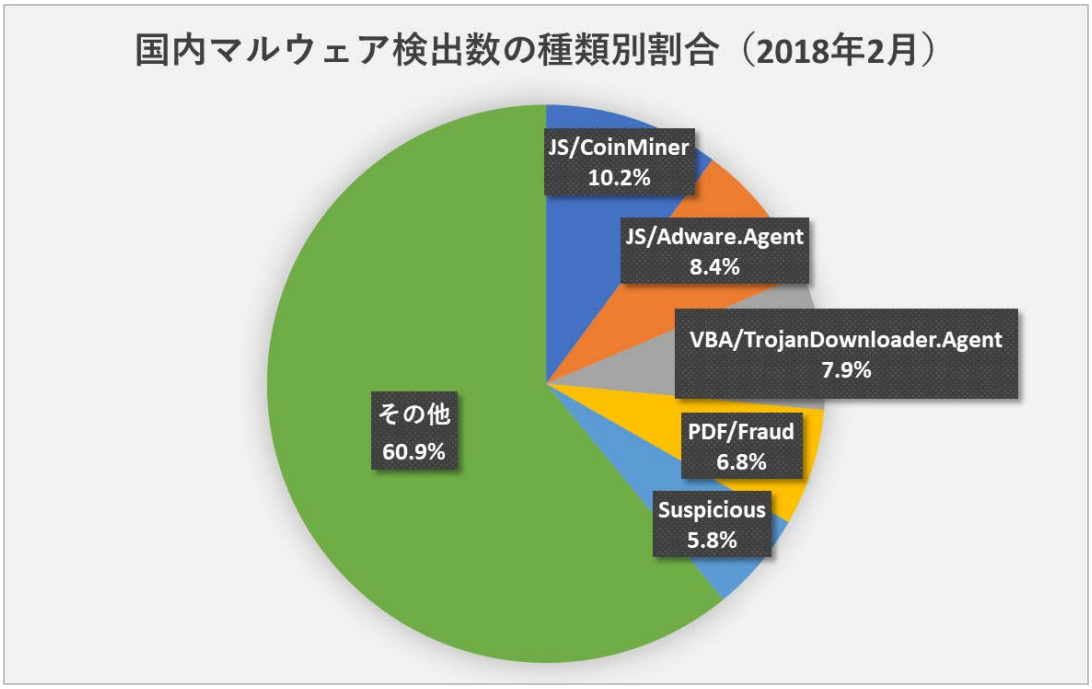
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 2 月マルウェア検出状況」

1. 2 月の概況について
2. バンキングマルウェア「Ursnif」感染を狙ったメール攻撃
3. Adobe Flash Player の脆弱性を突いた攻撃を確認

1. 2 月の概況について

2018 年 2 月 1 日から 2 月 28 日までの間、ESET 製品が国内で検出したマルウェアの種類別の割合は、以下のとおりです。



国内マルウェア検出数の比率（2018 年 2 月）

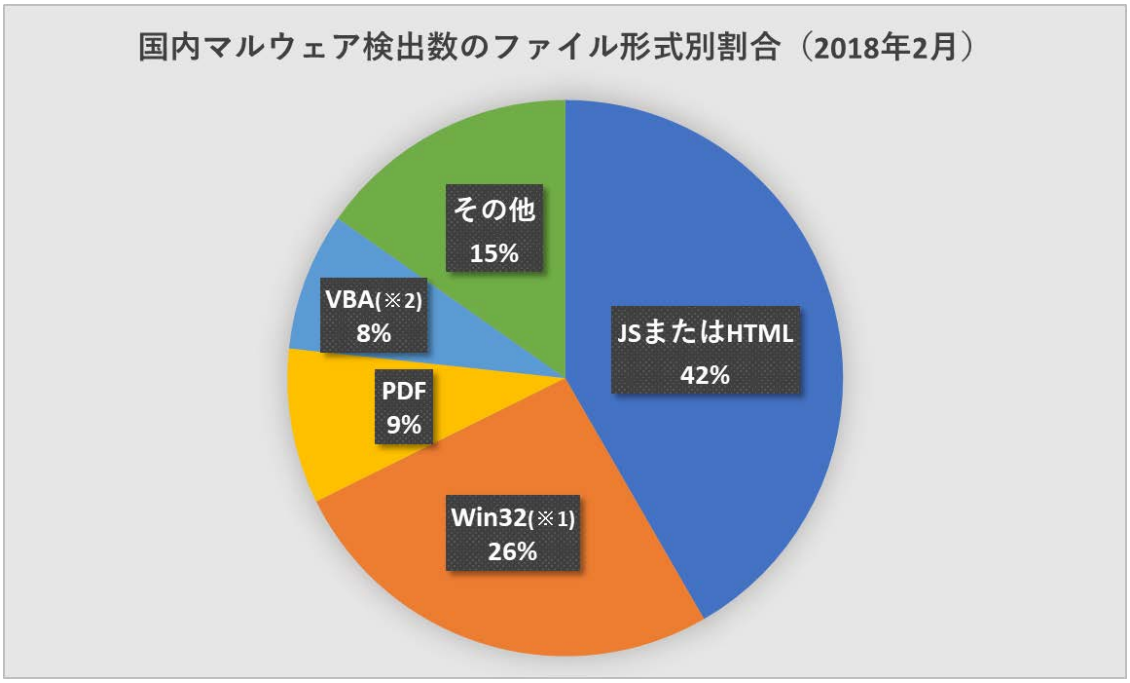
国内マルウェア検出数上位（2018 年 2月）

順位	マルウェア名	比率	種別
1	JS/CoinMiner	10.2%	マイニングスクリプト
2	JS/Adware.Agent	8.4%	アドウェア
3	VBA/TrojanDownloader.Agent	7.9%	ダウンローダー
4	PDF/Fraud	6.8%	詐欺サイトのリンクが埋め込まれた PDF
5	Suspicious	5.8%	未知の不審ファイル呼称
6	HTML/FakeAlert	5.1%	偽の警告文を表示するスクリプト
7	JS/Redirector	4.7%	別のページに遷移させるスクリプト
8	HTML/IFrame	2.8%	別のページに遷移させるスクリプト
9	HTML/ScrInject	2.6%	埋め込まれた不正なスクリプト
10	HTML/Refresh	2.0%	別のページに遷移させるスクリプト

（※）Potentially Unwanted Application(望ましくない可能性のあるアプリケーション)：コンピューターの動作に悪影響を及ぼすことや、ユーザーが意図しない振る舞いなどをする可能性があるアプリケーション。

2 月の検出数 1 位は、1 月に引き続き、JavaScript 形式のマイニングスクリプト「CoinMiner」でした。4 位の PDF/Fraud は詐欺サイトへのリンクを含んだ PDF ファイルに対する検出名です。昨年はダウンローダー型のマルウェアが検出数の大半を占めていましたが、今年に入ってから Web ブラウザーを狙った攻撃やアドウェアなど、脅

威が多様化しています。それを示すように、2 月の上位 10 種のうち 7 種は Web ブラウザーを実行環境とするもの（JS/や HTML/で始まる検出名）でした。これらの脅威は Windows PC だけではなく、Web ブラウザーを搭載しているあらゆるプラットフォームが攻撃の対象となります。



国内マルウェア検出数のファイル形式別割合（2018 年 2 月）

※1 32 ビットの Windows OS で動作するマルウェアの形式。64 ビット OS でも動作
※2 Microsoft Office のマクロを悪用したマルウェアの形式

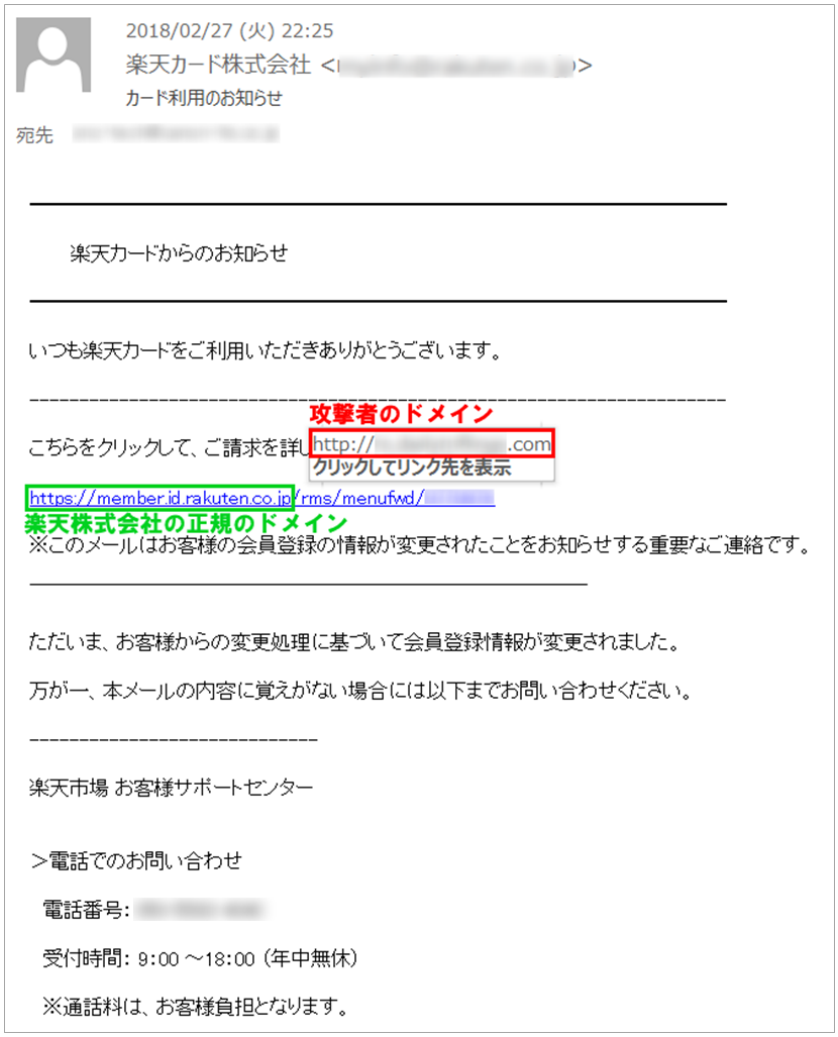
2. バンキングマルウェア「Ursnif」感染を狙ったメール攻撃

バンキングマルウェア「Ursnif」の感染を狙ったメールが多く確認されています。「Ursnif」は、インターネットバンキングサイトの認証情報（ユーザ ID やパスワード等）やクレジットカード情報を窃取します。感染した場合、銀行口座からの不正送金やクレジットカードの不正利用などの被害に遭う可能性があり、警視庁や日本サイバー犯罪対策センターはじめ他のベンダーからも、多くの注意喚起が出ています。

一般財団法人 日本サイバー犯罪対策センター 注意喚起情報
「インターネットバンキングマルウェアに感染させるウイルスメールに注意 」

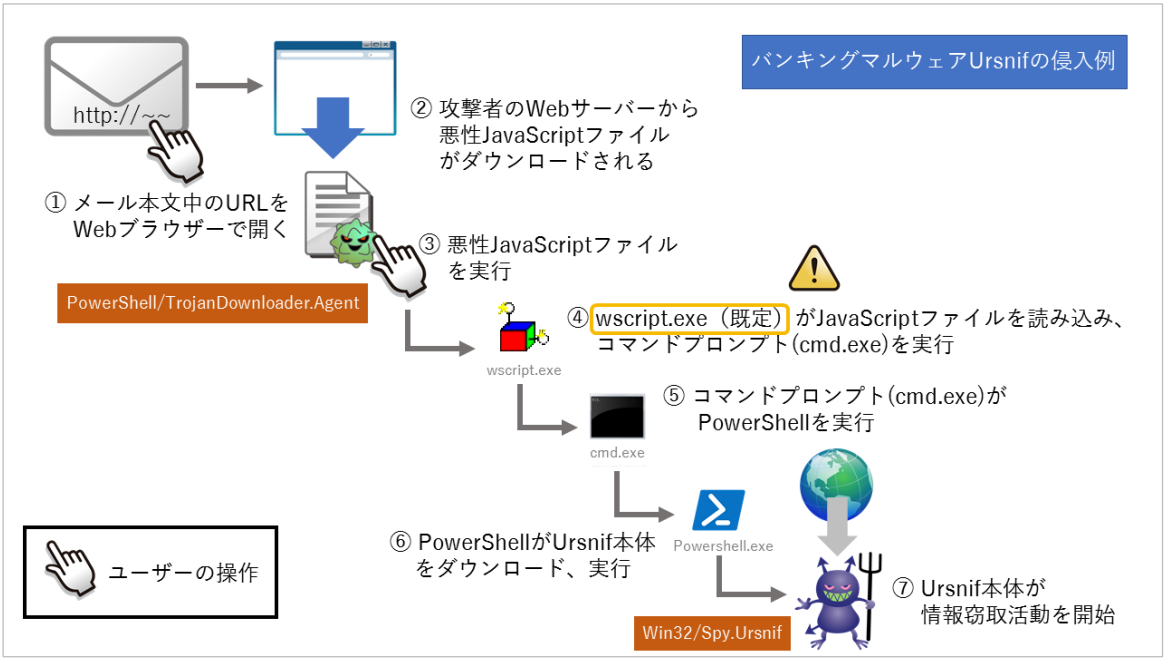
「Ursnif」の感染を狙ったメール攻撃には大きく分けて 2 種類あります。1 つ目は Microsoft Office のマクロ機能を悪用し「Ursnif」のダウンローダーをメールに添付しているパターンで、ESET 製品では「VBA/TrojanDownloader.Agent 」として検出します。2 つ目は本文中に「Ursnif」のダウンローダーの URL を記載しているパターンです。今回は 2 つ目のパターンについて詳しくご紹介します。

次の画像は楽天カードを騙り、「Ursnif」のダウンロード用 URL を記載したメールの例です。



楽天カードを騙ったメールの例

本文中のリンクは、一見すると楽天株式会社の正規のドメインのように見えますが、実際には攻撃者のドメインにアクセスするよう設定されています。このリンクをクリックすると、悪性の JavaScript ファイルがダウンロードされ、ファイルを実行すると「Ursnif」に感染します。



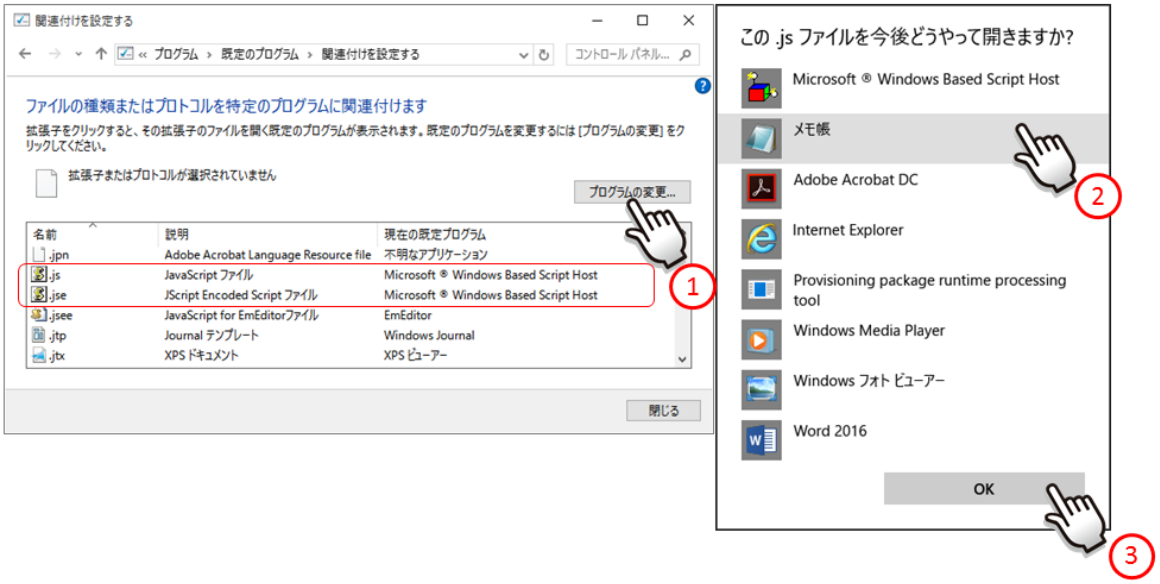
バンキングマルウェア「Ursnif」感染までの流れ

ESET 製品では、この悪性 JavaScript ファイルを「PowerShell/TrojanDownloader.Agent」として、Ursnif 本体を「Win32/Spy.Ursnif」としてそれぞれ検出し脅威を防ぎます。

感染のステップで使われる 3 つのプログラム（図中④wscript.exe、同⑤cmd.exe、同⑥powershell.exe）はいずれも Windows に標準で搭載されている正規のプログラムです。PowerShell はコマンドプロンプトより高度な処理を行うことができるため、悪用される事例が増加しています。

wscript.exe は Windows で JavaScript ファイル（拡張子.js または.jse）を実行するための既定のプログラムとして設定されています。この既定のプログラムをメモ帳などのテキストエディタに変更しておくとファイルが開かれてもスクリプトが実行されないため、感染を防ぐことができます。Windows 上で JavaScript ファイルを実行しない場合は、設定変更を推奨します。

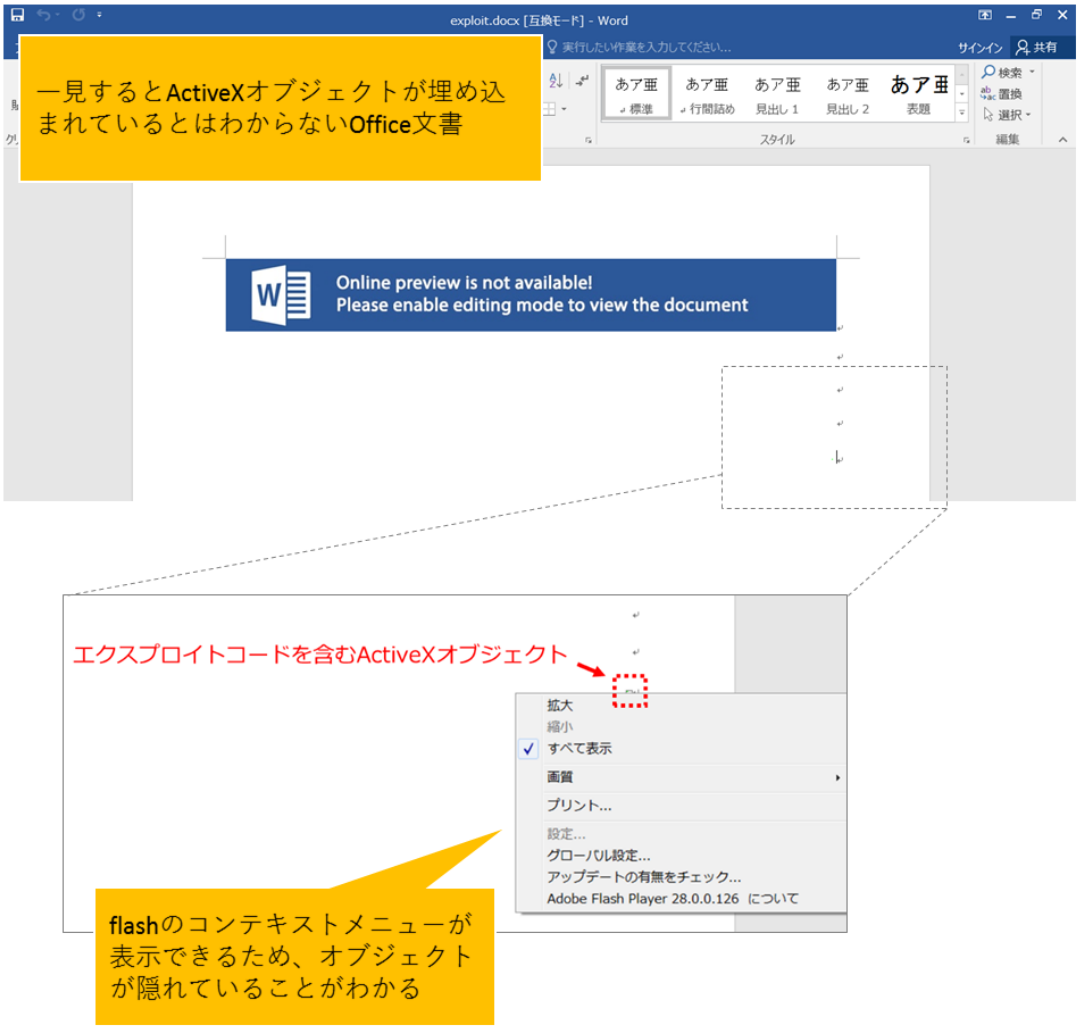
JavaScript ファイルを開く既定のプログラムは一般的に、（Windows10 の場合）スタートボタンを右クリック > [コントロール パネル] > （[プログラム]） > [既定のプログラム] > [ファイルの種類またはプロトコルのプログラムへの関連付け] > 拡張子一覧から「.js」(「.jse」)を選択し [プログラムの変更] > プログラム名の一覧から「メモ帳」などのテキストエディタを選択、することで変更できます。
なお、この設定変更は、Web ブラウザー上における JavaScript の実行には影響しません。



既定のプログラムの設定変更

3. Adobe Flash Player の脆弱性を突いた攻撃を確認

Adobe Flash Player の脆弱性（CVE-2018-4878）を悪用した攻撃が確認されています。ある事例では、この脆弱性を悪用するエクスプロイトコードが Microsoft Office ファイルに埋め込まれており、ファイルを開いただけで攻撃者によって仕組まれたプログラム（攻撃者サーバーとの通信、別のマルウェアのダウンロード）が実行されます。



エクスプロイトコードを含んだ Microsoft Word ファイル

この脆弱性に対する アドビ システムズ社のセキュリティアップデート は既に公開されています。未適用の場合、速やかに適用されることを推奨します。また、ESET 製品では、この脅威を「SWF/Exploit.CVE-2018-4878」として検出し脅威を防ぎます。

ご紹介したように、2 月はバンキングマルウェア「Ursnif」の感染を狙った攻撃や Adobe Flash Player の脆弱性を悪用した攻撃が確認されました。常に最新の脅威情報をキャッチアップすることが重要です。

■ 常日頃からリスク軽減するための対策について

各記事でご案内しているようなリスク軽減の対策をご案内いたします。
下記の対策を実施してください。

1. ESET 製品プログラムのウイルス定義データベースを最新にアップデートする

ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しております。
最新の脅威に対応できるよう、ウイルス定義データベースを最新にアップデートしてください。

2. OS のアップデートを行い、セキュリティパッチを適用する

ウイルスの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。
「Windows Update」などの OS のアップデートを行い、脆弱性を解消してください。

3. ソフトウェアのアップデートを行い、セキュリティパッチを適用する

ウイルスの多くが狙う「脆弱性」は、Java、Adobe Flash Player、Adobe Reader などのアプリケーションにも含まれています。
各種アプリのアップデートを行い、脆弱性を解消してください。

4. データのバックアップを行っておく

万が一ウイルスに感染した場合、コンピューターの初期化（リカバリー）などが必要になることがあります。 念のため、データのバックアップを行っておいてください。

5. 脅威が存在することを知る

「知らない人」よりも「知っている人」の方がウイルスに感染するリスクは低いと考えられます。ウイルスという脅威に触れてしまう前に「疑う」ことができるからです。
弊社を始め、各企業・団体からセキュリティに関する情報が発信されています。このような情報に目を向け、「あらかじめ脅威を知っておく」ことも重要です。

Canon
キヤノン ITソリューションズ株式会社

eset-info.canon-its.jp/